CLAIMS

Sub B1

1. An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking bits dependent on a plaintext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from a ciphertext before the ciphertext is output.

2. An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking intermediate bit data within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask $\underline{a}$ from the intermediate bit data masked by said masking means.

3. An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

data translation means for performing data translation to intermediate data within said apparatus;

means for randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

means for masking an input to said data translation means with the mask patterns selected by said selection means; and

means for removing an influence of the mask $\underline{a}$ from an output from said data translation means which is masked by said masking means.

4. An apparatus according to claim 1, wherein said means for masking the bits dependent on the plaintext within said apparatus with the selected mask patterns and said means for removing the influence of the mask $\underline{a}$ from the ciphertext comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

5. An apparatus according to claim 2, wherein said means for masking the intermediate bit data within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

6. An apparatus according to claim 3, wherein said data translation means, said means for masking the input to said data translation means with the selected mask patterns, and said means for removing the influence of the mask a from the masked output from said data translation means comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

7. An apparatus according to claim 3, further comprising:

first storage means for storing, in the form of a table, said means for randomly selecting one pattern of each of the pairs $a_i, \overline{a_i}$ (where i is a positive integer not less than one) of one or the plurality of predetermined mask patterns and the mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed, said means for masking the input to said data translation means

with the mask patterns ai, and said means for removing the influence of the masks ai from the masked output from said data translation means;

second storage means for storing, in the form of a table, said means for masking the input to said data translation means with mask patterns $\overline{a}$, and said means for removing an influence of the masks $\overline{a}$ from the masked output from said data translation means; and

masked data translation means for randomly selecting one of said first and second storage means every time encryption is performed, and performing the processing by said data translation means for masked data.

8. An apparatus according to claim 1, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion comprises a pair $a, \overline{a}$ of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns.

9. An apparatus according to claim 1, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed.

10. An apparatus according to claim 1, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and the Hamming weight H(a) of the mask $\underline{a}$ satisfies $0 < H(a) < n$.

11. An apparatus according to claim 1, wherein

a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and an absolute value of a difference between the Hamming weight H(a) of the mask $\underline{a}$ and a Hamming weight $H(\overline{a})$ of bit inversion $\overline{a}$ of the mask $\underline{a}$ is less than n/2.

12. A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs $a_i, \overline{a_i}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

means for masking bits dependent on a ciphertext within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask $\underline{a}$ from a plaintext before the plaintext is output.

13. A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs $a_i, \overline{a_i}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption

is performed;

means for masking intermediate bit data within said apparatus with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from the intermediate bit data masked by said masking means.

14. A decryption apparatus for converting a ciphertext block into a plaintext block depending on supplied key information, comprising:

data translation means for performing data translation to intermediate data within said apparatus;

means for randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

means for masking an input to said data translation means with the mask patterns selected by said selection means; and

means for removing an influence of the mask a from an output from said data translation means which is masked by said masking means.

15. An apparatus according to claim 12, wherein said means for masking the bits dependent on the plaintext within said apparatus with the selected mask patterns and said means for removing the influence of

the mask a from the ciphertext comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

16. An apparatus according to claim 13, wherein said means for masking the intermediate bit data within said apparatus with the selected mask patterns and said means for removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus w, and multiplication or division with respect to the modulus w.

17. An apparatus according to claim 15, wherein said data translation means, said means for masking the input to said data translation means with the selected mask patterns, and said means for removing the influence of the mask a from the masked output from said data translation means comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

18. An apparatus according to claim 14, further comprising:

first storage means for storing, in the form of a table, said means for randomly selecting one pattern of each of the pairs $a_i, \overline{a_i}$ (where i is a positive integer not less than one) of one or the plurality of

predetermined mask patterns and the mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed, said means for masking the input to said data translation means with the mask patterns ai, and means for removing the influence of the masks ai from the masked output from said data translation means;

second storage means for storing, in the form of a table, means for masking the input to said data translation means with mask patterns $\overline{a}$, and means for removing an influence of the masks $\overline{a}$ from the masked output from said data translation means; and

masked data translation means for randomly selecting one of said first and second storage means every time decryption is performed, and performing the processing by said data translation means for masked data.

19. An apparatus according to claim 12, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion comprises a pair $a, \overline{a}$ of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns.

20. An apparatus according to claim 13, wherein the pair $ai, \overline{ai}$ of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed.

21. An apparatus according to claim 12, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and the Hamming weight H(a) of the mask $\underline{a}$ satisfies $0 < H(a) < n$.

22. An apparatus according to claim 12, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and an absolute value of a difference between the Hamming weight H(a) of the mask $\underline{a}$ and a Hamming weight $H(\overline{a})$ of bit inversion $\overline{a}$ of the mask $\underline{a}$ is less than n/2.

23. An encryption method of converting a plaintext block into a ciphertext block depending on supplied key information, comprising the steps of:

randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

masking bits dependent on a plaintext within the method with the selected mask patterns; and

removing an influence of the mask $\underline{a}$ from a ciphertext before the ciphertext is output.

24. An encryption method of converting a plaintext block into a ciphertext block depending on supplied key information, comprising the steps of:

randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

masking intermediate bit data within the method with the selected mask patterns; and

removing an influence of the mask a from the masked intermediate bit data.

25. An encryption method of converting a plaintext block into a ciphertext block depending on supplied key information, comprising the steps of:

performing data translation to intermediate data within the method;

randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

masking an input to the data translation step with the selected mask patterns; and

removing an influence of the mask a from a masked output from the data translation step.

26. A method according to claim 23, wherein the step of masking the bits dependent on the plaintext

within the method with the selected mask patterns and the step of removing the influence of the mask a from the ciphertext comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

27. A method according to claim 24, wherein the step of masking the intermediate bit data within the method with the selected mask patterns and the step of removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

28. A method according to claim 25, wherein the data translation step, the step of masking the input to the data translation step with the selected mask patterns, and the step of removing the influence of the mask a from the masked output from the data translation step comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

29. A method according to claim 25, further comprising the steps of:

storing, in the form of a table, the step of randomly selecting one pattern of each of the pairs $a_i, \overline{a_i}$ (where i is a positive integer not less than one) of one or the plurality of predetermined mask patterns and the mask patterns obtained by bit

inversion of the predetermined mask patterns every time encryption is performed, the step of masking the input to said data translation step with the mask patterns ai, and the step of removing the influence of the masks ai from the masked output from the data translation step;

storing, in the form of a table, the step of masking the input to said data translation step with mask patterns $\overline{a}$, and step of removing an influence of the masks $\overline{a}$ from the masked output from the data translation step; and

randomly selecting one of the first and second storage steps every time encryption is performed, and performing the processing in the data translation step for masked data.

30. A method according to claim 23, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion comprises a pair $a, \overline{a}$ of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns.

31. A method according to claim 23, wherein that the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed.

32. A method according to claim 23, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and the Hamming weight H(a) of the mask $\underline{a}$ satisfies

$0 < H(a) < n$.

33. A method according to claim 23, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and an absolute value of a difference between the Hamming weight H(a) of the mask $\underline{a}$ and a Hamming weight $H(\overline{a})$ of bit inversion $\overline{a}$ of the mask $\underline{a}$ is less than n/2.

34. A decryption method of converting a ciphertext block into a plaintext block depending on supplied key information, comprising the steps of:

randomly selecting one pattern of each of pairs $a_i, \overline{a_i}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

masking bits dependent on a ciphertext within the method with the selected mask patterns; and

removing an influence of the mask $\underline{a}$ from a plaintext before the plaintext is output.

35. A decryption method of converting a ciphertext block into a plaintext block depending on supplied key information, comprising the steps of:

randomly selecting one pattern of each of pairs $a_i, \overline{a_i}$ (where $\underline{i}$ is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of

the predetermined mask patterns every time decryption is performed;

masking intermediate bit data within the method with the selected mask patterns; and

removing an influence of the mask a from the masked intermediate bit data.

36. A decryption method of converting a ciphertext block into a plaintext block depending on supplied key information, comprising the steps of:

performing data translation to intermediate data within the method;

randomly selecting one pattern of each of pairs $ai, \overline{ai}$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed;

masking an input to the data translation step with the selected mask patterns; and

removing an influence of the mask a from a masked output from the data translation step.

37. A method according to claim 34, wherein that the step of masking the bits dependent on the ciphertext within the method with the selected mask patterns and the step of removing the influence of the mask a from the plaintext comprise one of an exclusive OR, addition or subtraction with respect to a modulus W,

and multiplication or division with respect to the modulus w.

38. A method according to claim 35, wherein the step of masking the intermediate bit data within the method with the selected mask patterns and the step of removing the influence of the mask a from the masked intermediate bit data comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

39. A method according to claim 36, wherein the data translation step, the step of masking the input to the data translation step with the selected mask patterns, and the step of removing the influence of the mask a from the masked output from the data translation step comprise one of an exclusive OR, addition or subtraction with respect to a modulus, and multiplication or division with respect to the modulus.

40. A method according to claim 36, further comprising the steps of:

storing, in the form of a table, the step of randomly selecting one pattern of each of the pairs $a_i, \overline{a_i}$ (where i is a positive integer not less than one) of one or the plurality of predetermined mask patterns and the mask patterns obtained by bit inversion of the predetermined mask patterns every time decryption is performed, the step of masking the input to said data translation step with the mask patterns ai,

and the step of removing the influence of the masks ai from the masked output from the data translation step;

storing, in the form of a table, the step of masking the input to said data translation step with mask patterns $\overline{a}$, and step of removing an influence of the masks $\overline{a}$ from the masked output from the data translation step; and

randomly selecting one of the first and second storage steps every time decryption is performed, and performing the processing in the data translation step for masked data.

41. A method according to claim 34, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion comprises a pair $a, \overline{a}$ of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns.

42. A method according to claim 34, wherein the pair $a, \overline{a}$ of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed.

Sub A11 ~~43. A method according to claim 34, wherein~~ a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and the Hamming weight H(a) of the mask $\underline{a}$ satisfies $0 < H(a) < n$.

44. A method according to claim 34, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and

an absolute value of a difference between the Hamming weight H(a) of the mask a and a Hamming weight H($\bar{a}$) of bit inversion $\bar{a}$ of the mask a is less than n/2.

45. A computer-usable program storage medium storing computer-readable program code means for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

computer-readable program code means for causing a computer to randomly select one pattern of each of pairs $a_i, \bar{a}_i$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of the predetermined mask patterns every time encryption is performed;

computer-readable program code means for causing said computer to mask bits dependent on a plaintext within the method with the selected mask patterns; and

computer-readable program code means for causing said computer to remove an influence of the mask a from a ciphertext before the ciphertext is output.

46. An encryption apparatus for converting a plaintext block into a ciphertext block depending on supplied key information, comprising:

means for randomly selecting one pattern of each of pairs $a_i, \bar{a}_i$ (where i is a positive integer not less than one) of one or a plurality of predetermined mask patterns and mask patterns obtained by bit inversion of

the predetermined mask patterns every time encryption is performed;

means for masking bits dependent on a key within said apparatus with the mask patterns selected by said selection means;

data translation means for converting intermediate data within said apparatus with the key; and

means for removing an influence of the mask $\underline{a}$ from an output from said data translation means.

47. An apparatus according to claim 46, wherein the pair $a, \bar{a}$ of the mask patterns and the mask patterns obtained by bit inversion comprises a pair $a, \bar{a}$ of predetermined fixed mask patterns and mask patterns obtained by bit inversion of the fixed mask patterns.

48. An apparatus according to claim 46, wherein the pair $a, \bar{a}$ of the mask patterns and the mask patterns obtained by bit inversion are not necessarily concealed.

49. An apparatus according to claim 46, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and the Hamming weight H(a) of the mask $\underline{a}$ satisfies $0 < H(a) < n$.

50. An apparatus according to claim 46, wherein a Hamming weight indicating the number of bits "1s" of an n-bit long bit sequence $\underline{x}$ is defined as H(x), and

an absolute value of a difference between the Hamming weight H(a) of the mask $\underline{a}$ and a Hamming weight $H(\bar{a})$ of bit inversion $\bar{a}$ of the mask $\underline{a}$ is less than n/2.

ADD A12